EXECUTIVE SUMMARY

The following plan represents the third generation of the Department of Energy (DOE) Cyber Security Action Plan. This plan defines the Office of Cyber Security strategic vision of becoming a national center of excellence for the safeguarding of classified and unclassified information on electronic systems and critical cyber infrastructures. This enormous undertaking encompasses policies, procedures, and implementation efforts throughout a large, diverse, and geographically dispersed organization. The Action Plan lays out a concrete set of projects over a 2-year period.

This plan supports four functional areas and three key goals. These four areas are as follows:

- Planning and Performance Management
- Education, Training, and Awareness
- Engineering and Assessments
- Technical Development.

The three goals are as follows:

- Strengthening the cyber security community
- Strengthening the implementation of DOE's cyber security policies to meet or exceed national standards
- Strengthening the DOE internal cyber security infrastructure

To achieve the goals of the Office of Cyber Security, the following action items will be undertaken over the next 2-year period:

- Continue with the development of the action plan to promote and support DOE's vision.

- Define roles and responsibilities for Headquarters and line organizations.

- Ensure that E-government initiatives are secure and responsive to the public.

- Update the agencywide Cyber Security Threat Statement including new threat information based on recent world events.

- Deploy a DOE-wide performance metrics program to provide an assessment of real-time implementation of cyber security programs and to improve security policies where enhancement is warranted.

- Develop and now maintain and update the Government Information Security Reform Act (GISRA) Plan of Action and Milestones (POA&M) for OMB. This report describes the Chief Information Officer's (CIO) plan to strengthen DOE's cyber security program by ensuring weaknesses identified by internal and external audits are tracked from identification to resolution.

- Develop a cyber security information technology (IT) capital planning process to ensure cyber security dollars are appropriately managed, reviewed, and funded to facilitate the full

integration of security into the IT life cycle.

- Continue with the evolution of DOE cyber security guidance directives.
- Expand the Outreach/Lessons Learned program with the continued publication of the CIO's Office of Cyber Security Cyber Security Daily New Brief and publication of the "best practices" papers.
- Develop and expand a comprehensive DOE-wide cyber training program, including forensics awareness training, a recognition program, and a catalog of courses.
- Continue to support the Computer Incident Advisory Capability (CIAC) in its mission to assist any DOE element that experiences a computer security incident by providing analysis, response, and restoration of operation.
- Expand public key infrastructure (PKI) capabilities throughout DOE to support trusted relationships among all users.
- Fund Secure Telephone Unit-Third Generation (STU-III) replacement at 25 percent of assets annually over the next 4 years.
- Continue to fund DOE-wide infrastructure/architecture upgrades.
- Fund innovative technologies to ensure practical and enhanced cyber security protection capabilities.
- Transition a Counterintelligence project (Intrusion Monitoring Analysis and Correction [IMAC]) that improves the ability to forecast upcoming attacks to the Office of Cyber Security.
- Continue with Step 2 of the Project Matrix Initiative.